2025年春季学期第二次作业

1. 设 $f(x)=a_nx^n+\cdots+a_1x+a_0\in\mathbb{Z}[x]$. 若 $\alpha=\frac{k}{l}\in\mathbb{Q}$, $\gcd(k,l)=1$ 为其根, 证明: $k\mid a_0$ 且 $l\mid a_n$.

2. 设 D 是 UFD, $a,b_1,\dots b_n\in D^*$. 证明: 如果 $\gcd(a,b_i)=1$, $i=1\dots n$, 则

$$\gcd(a,\ b_1\cdots b_n)=1.$$

3. 判断整系数多项式 x^2+4, x^3+4, x^4+4 和 $x^5+12x^3+36x+12$ 在 $\mathbb{Q}[x]$ 中是否不可约.

4. 已知 $f(x)=x^p-x-1$ 在 $\mathbb{Z}_p[x]$ 中不可约, 其中 p 为素数. 证明:

$$f(x)=x^p-x-1\quad 和\quad g(x)=x^p+(p-1)x+p-1$$

在 $\mathbb{Q}[x]$ 上不可约.

提示: 利用环同态:

$$\begin{array}{rccc}\phi_p: & \mathbb{Z}[x] & \longrightarrow & \mathbb{Z}_p[x]\\ & \sum_i a_ix^i & \mapsto & \sum_i \bar{a}_ix^i.\end{array}$$

5. 设 $f(x)$ 是无穷阶可导的实函数, 其导数记为 f', k 阶导数记为 $f^{(k)}$.

(a) 设 $f\in\mathbb{R}[x]$. 证明: f,f',f'' 在 $\mathbb{R}$ 上线性无关当且仅当 $\deg(f)\geq 2$.

(b) 设 $f(x)=x^2e^x$. 求最小正整数 n 使得 $f,f',\dots,f^{(n)}$ 在 $\mathbb{R}$ 上线性相关.

注: 有些同学第一题证法:

$$f(x)=(lx-k)g(x)$$

设 $g(x)=b_{n-1}x^{n-1}+\cdots+b_0$ 则有 $l\cdot b_{n-1}=a_n$ 且 $-kb_0=a_0$

$\Rightarrow l\mid a_n$ 且 $k\mid a_0$

问题: 为什么 $g(x)$ 一定整系数! 没有用到 $\gcd(l,k)=1$ 条件.

正确证法: $f(x)=(lx-k)(b_{n-1}x^{n-1}+\cdots+b_0)$

若 $\exists i\in\{1,\dots,n-1\}$, b_i 非整, 则 对 $b_{n-1}x^{n-1}+\cdots+b_0$ 通分得到的公母 d, 因为 $f(x)\in\mathbb{Z}[x]$

所以 $d\mid(lx-k)$ 则 $d\mid l$ 且 $d\mid k\Rightarrow d\mid\gcd(l,k)=1$ $\rightarrow\leftarrow$

所以 $b_i\in\mathbb{Z}$ $\forall i\in\{1,\dots,n-1\}$, 由 $lb_{n-1}=a_n$ 且 $-kb_0=a_0$ 得 $l\mid a_n$, $k\mid a_0$ □

1. 设 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. 若 $\alpha = \frac{k}{l} \in \mathbb{Q}$, $\gcd(k,l) = 1$ 为其根, 证明: $k \mid a_0$ 且 $l \mid a_n$.

Pf:

$f(\alpha) = f(\frac{k}{l}) = a_n(\frac{k}{l})^n + \cdots + a_1(\frac{k}{l}) + a_0 = 0$

$\Rightarrow \frac{a_n k^n + \cdots + a_1 k \cdot l^{n-1} + a_0 l^n}{l^n} = 0$

$\Rightarrow a_n k^n + \cdots + a_1 k \cdot l^{n-1} + a_0 l^n = 0$

$\Rightarrow a_n k^n + \cdots + a_1 k \cdot l^{n-1} = -a_0 l^n$

$\Rightarrow k \mid LHS \Rightarrow k \mid RHS$ 又因为 $\gcd(k,l)=1$

所以 $k \mid a_0$

另外面 $a_n k^n = -a_{n-1} k^{n-1} l - \cdots - a_1 k l^{n-1} - a_0 l^n$

$l \mid RHS \Rightarrow l \mid a_n k^n$ 又因为 $\gcd(k,l)=1$

所以 $l \mid a_n$. □

2. 设 D 是 UFD, $a, b_1, \ldots b_n \in D^*$. 证明: 如果 $\gcd(a, b_i) = 1$, $i = 1 \ldots n$, 则

$$\gcd(a,\ b_1 \cdots b_n) = 1.$$

Pf:

反证法: 若 $\gcd(a, b_1 \cdots b_n) \neq 1$, 则 $\exists\, g \in D \setminus U_D$ s.t. $\gcd(a, b_1 \cdots b_n) = g$

则 $g \mid a$ 且 $g \mid b_1 \cdots b_n$, 设 p 是 g 的不可约因子. 则 $p \mid g$ 且

$p \mid b_1 \cdots b_n$, 因为 UFD 中不可约元是素元, 所以 存在 $i \in [1, n]$ s.t. $p \mid b_i$

$p \mid a$ 且 $p \mid b_i$ 与 $\gcd(a, b_i) = 1$ 矛盾. □

3. 判断整系数多项式 x^2+4, x^3+4, x^4+4 和 $x^5+12x^3+36x+12$ 在 $\mathbb{Q}[x]$ 中是否不可约.

Pf: 待定系数法

对 x^2+4: 设 $x^2+4=(x+a)(x+b)$, $a,b\in\mathbb{Q}$, 则 $x^2+4=x^2+(a+b)x+ab$

$\Rightarrow a+b=0$ 且 $ab=4$

$a=-b$ 且 $-b^2=4$ $\rightarrow\leftarrow$ $b\in\mathbb{Q}$

所以 x^2+4 不可约.

x^3+4: 若 x^3+4 在 $\mathbb{Q}$ 内可约, 则 x^3+4 至少有一个一次因子.

设 $x^3+4=(x+a)(x^2+cx+d)$

$=x^3+cx+dx+ax^2+acx+ad$

$=x^3+(c+a)x^2+(d+ac)x+ad$.

$\Rightarrow \begin{cases} a+c=0 \\ d+ac=0 \\ ad=4 \end{cases} \Rightarrow \begin{array}{l} a=-c \\ d-c^2=0 \Rightarrow d=c^2 \\ ad=(-c)\cdot c^2=4 \Rightarrow -c^3=4 \end{array}$

$-c^3=4$ 在 $\mathbb{Q}$ 中无解.

x^4+4: 则 $x^4+4=(x^2+bx+c)(x^2+ex+f)$

或 $x^4+4=(x+k)(x^3+mx^2+nx+i)$

$x^4+4=x^4+ex^3+fx^2+bx^3+bex^2+bfx+cx^2+cex+cf$

$=x^4+(e+b)x^3+(f+be+c)x^2+(bf+ce)x+cf$

$$\Rightarrow \begin{cases} e+b=0 \\ f+be+c=0 \\ bf+ce=0 \\ cf=4 \end{cases} \Rightarrow \begin{cases} e=-b \\ f-b^2+c=0 \\ bf-bc=0 \\ cf=4 \end{cases} \Rightarrow \begin{cases} f+c=b^2 \\ b(f-c)=0 \\ cf=4 \end{cases}$$

若 $b=0$ 则 $f+c=0$ 由 $cf=4 \to \in$

若 $f=c$ 则 $2c=b^2 \Rightarrow c=\frac{b^2}{2}$ 由 $c^2=4 \Rightarrow c=\pm 2$

同当 $c=\frac{b^2}{2}$ 仅当时 $\Rightarrow c=2$ 则 $f=c=2$

$b^2=2\cdot c=4 \Rightarrow b=\pm 2 \Rightarrow e=-b=\mp 2$

则 $x^4+4=(x^2+2x+2)(x^2-2x+2)$

或 $x^4+4=x^4+mx^3+nx^2+ix+k x^3+kmx^2+knx+ki$

$=x^4+(m+k)x^3+(n+km)x^2+(i+kn)x+ki$

$$\Rightarrow \begin{cases} m+k=0 \\ n+km=0 \\ i+kn=0 \\ ki=4 \end{cases} \Rightarrow \begin{cases} m=-k \\ n-k^2=0 \\ i+kn=0 \\ ki=4 \end{cases} \Rightarrow \begin{cases} m=-k \\ n=k^2 \\ i+k^3=0 \\ k\cdot i=4 \end{cases} \Rightarrow \begin{cases} m=-k \\ n=k^2 \\ i=-k^3 \\ -k^4=4 \end{cases}$$

$k^4=-4$，不存在这样的 $k\in R$.

或者 $x^4+4=x^4+4x^2+4-4x^2=(x^2+2)^2-4x^2=(x^2+2+2x)(x^2+2-2x)$

$x^5+12x^3+36x+12$：3不1，3|12，3|36，$3^2=9\nmid 12$

所以 $x^5+12x^3+36x+12$ 在 $\mathbb{Q}[A]$ 上不可约.

□

判断多项式不可约的方法：

①试根法：用于判断多项式是否有一次因式：

命题：

. 设 $f(x)=a_nx^n+\cdots+a_1x+a_0\in\mathbb{Z}[x]$. 若 $\alpha=\frac{k}{l}\in\mathbb{Q}$, $\gcd(k,l)=1$ 为其根，
证明: $k\mid a_0$ 且 $l\mid a_n$.

推论：$f(x)$ 可能的有理根只有有限多个.

推论：次数 n 不等于 1 次的多项式 $f(x)\in\mathbb{Z}[x]$ 在 $\mathbb{Q}[x]$ 上不可约，当且仅当 $f(x)$ 没有有理根.

例：x^2+4：$k\mid 4$　$l\mid 1$，

可能的有理根：±4　±2　±1

代入均非 x^2+4 的根 $\Rightarrow$ x^2+4 在 $\mathbb{Q}[x]$ 中不可约.

或 $x^2+4=(x+2i)(x-2i)$ 无有理根

x^3+4：　$k\mid 4$　$l\mid 1$

可能的有理根：±4, ±2, ±1

代入都不是 x^3+4 的根　$\Rightarrow$ x^3+4 在 $\mathbb{Q}[x]$ 中不可约.

或 $x^3+4=x^3+(4^{\frac{1}{3}})^3=(x+4^{\frac{1}{3}})(x^2-4^{\frac{1}{3}}x+4^{\frac{2}{3}})$

②：　艾森斯坦因判别法，

定理 6.37 *(Eisenstein 不可约性判别法)* 设

$$f=f_nx^n+f_{n-1}x^{n-1}+\cdots+f_0,$$

其中 $n>0$, $f_n,f_{n-1},\ldots,f_0\in\mathbb{Z}$ 且 $f_n\neq0$. 设 p 是素数.
如果

$$p\nmid f_n,\ p\mid f_{n-1},\ \ldots,\ p\mid f_0,\ p^2\nmid f_0,$$

则 f 在 $\mathbb{Q}[x]$ 中不可约.

③待定系数法：见上页

② 模 p 法：p 为素数：

$$\phi_p: \mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$$

$$\sum a_i x^i \longmapsto \sum \bar{a}_i x^i$$

命题！ 设 $f(x) \in \mathbb{Z}[x]$ 为本原多项式，若 p 不整除 $f(x)$ 的首项系数，且 $f(x)$ 模 p 后不可约，则 $f(x)$ 在 $\mathbb{Z}[x]$ 中不可约.

证明：反证. 设 $f(x)$ 在 $\mathbb{Z}[x]$ 中可约，则存在正次数多项式 $a(x), b(x) \in \mathbb{Z}[x]$ 且 $\deg(a(x)) < \deg(f(x))$, $\deg(b(x)) < \deg(f(x))$. 使得

$$f(x) = a(x) \cdot b(x)$$

因为 p 不整除 $lc(f)$ (:f 的首项系数)，

所以 $p \nmid lc(a)$ 且 $p \nmid lc(b)$

则 $\deg(\phi_p(a)) = \deg(a) > 0$ $\quad \deg(\phi_p(b)) = \deg(b) > 0$

$$\phi_p(f) = \phi_p(a) \cdot \phi_p(b)$$

$\therefore f(x)$ 在 $\mathbb{Z}_p[x]$ 中不可约矛盾. □

条件的多项重性：① 若 $f(x)$ 非本原多项式：eg：$f(x) = 5(x-1)$ 5在$\mathbb{Z}$中不是素元

所以 $5(x-1)$ 可以看做 $\mathbb{Z}[x]$ 中的不可约分解式. 取 $p=2$

$$\phi_2: \mathbb{Z}[x] \longrightarrow \mathbb{Z}_2[x]$$

$$5(x-1) \longmapsto x-1$$

可约　　不可约

② 若 $p \mid lc(f)$ eg: $f(x) = (2x-1)(x+1) \in \mathbb{Z}[x]$ 取 $p=2$

$$\phi_2: \mathbb{Z}[x] \longrightarrow \mathbb{Z}_2[x]$$

$$(2x-1)(x+1) \longmapsto x+1$$

可约　　不可约

Question: 在$\mathbb{Z}[x]$中不可约是否等价于在$\mathbb{Q}[x]$中不可约？

回顾 Gauss 引理：

定理 6.36 设 $f \in \mathbb{Z}[x]$ 且 $\deg(f) > 0$. 如果 f 不能写成两个 $\mathbb{Z}[x]$ 中正次数的多项式之积. 则 f 在 $\mathbb{Q}[x]$ 不可约.

注：$f(x)$在$\mathbb{Z}[x]$中不可约 $\neq$ $f(x)$不能写成两个$\mathbb{Z}[x]$中正次数的多项式之积

eg: $f(x)=2(x-1)$

可约 但不能写成两个正次数多项式之积.

若$f(x)$是本原多项式，则

$f(x)$在$\mathbb{Z}[x]$中不可约 $=$ $f(x)$不能写成两个$\mathbb{Z}[x]$中正次数多项式之积

推论! $f(x)$为本原多项式，则 $f(x)$在$\mathbb{Z}[x]$中不可约当且仅当 $f(x)$在$\mathbb{Q}[x]$中不可约.

证明：“$\Rightarrow$”定理6.36

“$\Leftarrow$”设$f(x)$在$\mathbb{Z}[x]$中可约，由$f(x)$是本原多项式可知，$f(x)$可以写成两个$\mathbb{Z}[x]$中正次数多项式之积，$\mathbb{Z}[x]$的多项式自然在$\mathbb{Q}[x]$中，所以$f(x)$在$\mathbb{Q}[x]$中可约 $\longrightarrow\longleftarrow$. □

4. 已知 $f(x) = x^p - x - 1$ 在 $\mathbb{Z}_p[x]$ 中不可约, 其中 p 为素数. 证明:

$$f(x) = x^p - x - 1 \quad \text{和} \quad g(x) = x^p + (p-1)x + p - 1$$

在 $\mathbb{Q}[x]$ 上不可约.

提示: 利用环同态:

$$\begin{array}{rccc} \phi_p: & \mathbb{Z}[x] & \longrightarrow & \mathbb{Z}_p[x] \\ & \sum_i a_i x^i & \mapsto & \sum_i \bar{a}_i x^i. \end{array}$$

$x^p=x$

$g(x) \mid f(x)$

$g(x^p) \mid f(x)$

$g(x^{p^2}) \mid f(x)$

证明：$f(x)$为本原多项式，由推论1，只需证$f(x)$在$\mathbb{Z}[x]$上不可约，又因为$p \nmid lc(f)$，由命题1知：$f(x)$在$\mathbb{Z}[x]$中不可约一定可以推出$f(x)$在$\mathbb{Z}[x]$上不可约。

$\varphi_p(g(x)) = x^p - x - 1$ 所以在 $\mathbb{Z}_p[x]$ 中 $g(x) = f(x)$，$f(x)$ 在 $\mathbb{Z}_p[x]$ 中不可约 $\Rightarrow$ $g(x)$ 在 $\mathbb{Z}_p[x]$ 中不可约，类似地我们有 $g(x)$ 在 $\mathbb{Q}[x]$ 上不可约

□

5. 设 $f(x)$ 是无穷阶可导的实函数, 其导数记为 f', k 阶导数记为 $f^{(k)}$.

(a) 设 $f \in \mathbb{R}[x]$. 证明: f, f', f'' 在 $\mathbb{R}$ 上线性无关当且仅当 $\deg(f) \geq 2$.

(b) 设 $f(x) = x^2 e^x$. 求最小正整数 n 使得 $f, f', \ldots, f^{(n)}$ 在 $\mathbb{R}$ 上线性相关.

Pf: (a): ($\Leftarrow$) $\deg(f) \geq 2$ 则 $\deg(f') \geq 1$ $\deg(f'') \geq 0$，且 $f'' \neq 0$

设 $f = a_n x^n + \cdots + a_0$ 则 $f' = n a_n x^{n-1} + \cdots + a_1$，$f'' = n a_n (n-1) x^{n-2} + \cdots + a_2$

若 $\exists\, c_1, c_2, c_3 \in \mathbb{R}$ 使得

$c_1 f + c_2 f' + c_3 f'' = 0$ 则

$\text{Weff}(x, n) = c_1 a_n = 0 \Rightarrow c_1 = 0$

$\text{Weff}(x, n-1) = c_1 a_{n-1} + c_2 \cdot n a_n = 0$

$\Rightarrow c_2 \cdot n a_n = 0 \Rightarrow c_2 = 0$

$\text{Weff}(x, n-2) = c_1 a_{n-2} + c_2 \cdot (n-1) a_{n-1} + c_3 n a_n (n-1) = 0$

$\Rightarrow c_3 a_n n(n-1) = 0 \Rightarrow c_3 = 0$

所以 f, f', f'' 线性无关.

($\Rightarrow$) 若 $\deg(f) = 2$, 则 $\deg(f') \leq 1$,

若 $\deg(f) = 1$, 则 $\deg(f') = 0$ $f'' = 0$

$0 \cdot f + 0 \cdot f' + C \cdot f'' = 0$ $\forall\, C \neq 0$

$\Rightarrow f, f', f''$ 线性相关.

若 $\deg(f) = 0$, 则 $f' = f'' = 0$

$\Rightarrow$ f, f', f'' 线性相关.

(b). $f(x)=x^2e^x$

$f'(x)=2xe^x+x^2\cdot e^x=(2x+x^2)e^x$

$f''(x)=(2+2x)e^x+(2x+x^2)e^x=(2+4x+x^2)e^x$

$f'''(x)=(4+2x)e^x+(2+4x+x^2)e^x$

$=(6+6x+x^2)e^x$

若 f, f' 在 $\mathbb{R}$ 上线性相关 则 $\exists\ C_1, C_2\in\mathbb{R}$ 不全为0, 使

$C_1f+C_2f'=0$

$C_1x^2e^x+C_2(2x+x^2)e^x=0 \Rightarrow C_1x^2+C_2(2x+x^2)=0$

$\Rightarrow \begin{cases} C_1+C_2=0 \\ 2C_2=0 \end{cases} \Rightarrow C_1=C_2=0$

若 f, f', f'' 在 $\mathbb{R}$ 上线性相关, 则 $\exists\ C_1, C_2, C_3\in\mathbb{R}$ 不全为0, 使

$C_1x^2+C_2(2x+x^2)+C_3(2+4x+x^2)=0$

$(C_1+C_2+C_3)x^2+(2C_2+4C_3)x+2C_3=0$

$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 4 \\ 0 & 0 & 2 \end{pmatrix}\vec{C}=\vec{0}$ 只有零解.

若 f, f', f'', f''' 线性相关, 则 $\exists\ C_1\ C_2\ C_3\ C_4$ 使

$C_1x^2+C_2(2x+x^2)+C_3(2+4x+x^2)+C_4(6+6x+x^2)=0$

$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 4 & 6 \\ 0 & 0 & 2 & 6 \end{pmatrix}\begin{pmatrix} C_1 \\ C_2 \\ C_3 \\ C_4 \end{pmatrix}$

$\Rightarrow c_1=1 \quad c_2=-3 \quad c_3=3 \quad c_p=-1$

$f-3f'+3f''-f'''=0$，所以最小阶 n 为 3. □

子空间直和分解

设 $V=W_1\oplus W_2\oplus\cdots\oplus W_m$ 是 m 个子空间的直和分解，那么 $\forall \vec{x}\in V$ 可以唯一地表为：

$$\vec{x}=\vec{x}_1+\vec{x}_2+\cdots+\vec{x}_m \quad \vec{x}_i\in W_i$$

设 $P_i: V\longrightarrow V$

$$x\longmapsto x_i$$

则 P_i 是 V 上的线性算子，此外还有

$$P_1+P_2+\cdots+P_m=\underbrace{\varepsilon}_{\text{单位映射 } \varepsilon: x\to x}$$

而且当 $i\neq j$ 时 $P_iP_j=0$，$P_i^2=P_i$

P_i 是 V 在 W_i 上的投影.

$$W_i=P_iV=\{P_i\vec{x}\mid \vec{x}\in V\}=\{\vec{x}\in V\mid P_i\vec{x}=\vec{x}\}$$

解释：$\forall \vec{y}\in W_i \quad P_i\vec{y}=\vec{y}$，另一边，若 $P_i\vec{y}=\vec{y}$ 则 $\vec{y}\in \mathrm{Im}\, W_i$.

$$K_i=\ker P_i=W_1+\cdots+W_{i-1}+W_{i+1}\cdots+W_m$$

Q：反过来呢？

若 $\sum P_i=\varepsilon$，$P_i^2=P_i \quad 1\le i\le m$；$P_iP_j=0$，$i\neq j$

是否有 $V=W_1\oplus\cdots\oplus W_m$，其中 W_i 为 $\mathrm{Im}\, P_i$

定理：设 $P_1 \cdots P_m : V \longrightarrow V$ 是满足下列条件的有限个线性映射的集合：

$$\sum_{i=1}^{m} P_i = \mathcal{E} \qquad P_i^2 = P_i \ (1 \le i \le m); \quad P_i P_j = O, \ i \neq j$$

那么 $V = W_1 \oplus \cdots \oplus W_m$

其中 $W_i = \mathrm{Im}\, P_i$

证明：对 $\forall \vec{x} \in V$,

$$\vec{x} = \mathcal{E}(\vec{x}) = (P_1 + \cdots + P_m)\cdot(\vec{x})$$

$$= P_1(\vec{x}) + P_2(\vec{x}) + \cdots + P_m(\vec{x})$$

其中 $P_i(\vec{x}) \in \mathrm{Im}\, P_i$

所以 $V = W_1 + W_2 + \cdots + W_m$

下证对 $\forall i$, $W_i \cap (W_1 + \cdots + W_{i-1} + W_{i+1} + \cdots + W_m) = \{\vec{0}\}$

不妨设 $i=1$, 下证 $W_1 \cap (W_2 + W_3 + \cdots + W_m) = \{\vec{0}\}$

任取 $\vec{y} \in W_1 \cap (W_2 + \cdots + W_m)$

只存在 $\vec{a}_1, \vec{a}_2, \cdots \vec{a}_m$ 使得

$$\vec{y} = P_1 \vec{a}_1 \text{ 且 } \vec{y} = P_2 \vec{a}_2 + \cdots + P_m \vec{a}_m$$

则 $P_1 \vec{y} = P_1^2 \vec{a}_1 = P_1 \vec{a}_1 = \vec{y}$

$$P_1 \vec{y} = P_1 P_2 \vec{a}_2 + \cdots + P_1 P_m \vec{a}_m = \vec{0}$$

所以 $\vec{y} = \vec{0}$ □

补充：为什么 x^p-x+1 在 $\mathbb{Z}_p[x]$ 上不可约？

Pf: 首先 x^p-x+1 没有不可约的单因子，因为 $0,1,\cdots p-1$ 都不是它的根，

设 x^p-x+1 在"更大域"中有根 α （$\alpha \notin \mathbb{Z}_p$）

（类似 x^2+1 在 $\mathbb{R}$ 中一定没有根在 $\mathbb{C}$ 中一定有根）

则 $(\alpha+1)^p-(\alpha+1)+1 = \alpha^p+1-\alpha-1+1 = \alpha^p-\alpha+1 = 0$

所以 $\alpha+1,\ \alpha+2,\cdots\ \alpha+p-1$ 都是 x^p-x+1 的根.

反证法：若 x^p-x+1 在 $\mathbb{Z}_p[x]$ 上可约，则存在 $g(x), h(x) \in \mathbb{Z}_p[x]$ 且

$1 < \deg(g(x)) < p-1$ ，$1 < \deg(h(x)) < p-1$

（1 是因为没有单因子）

使得 $x^p-x+1 = g(x)\cdot h(x)$

$= (x-\alpha)(x-(\alpha+1))(x-(\alpha+2))\cdots(x-(\alpha+p-1))$

说明 $g(x)$ 由2个或以上单因子乘积得到

简单来看，比如 $g(x) = (x-\alpha)(x-(\alpha+1))$

$= x^2-(\alpha+1)x-\alpha x+\alpha(\alpha+1)$

$= x^2-(2\alpha+1)x+\alpha(\alpha+1)$

此时 $g(x)$ 的次高项为 $-2\alpha-1$ 因为 $g(x) \in \mathbb{Z}_p[x]$

$\Rightarrow -2\alpha-1 \in \mathbb{Z}_p \Rightarrow -2\alpha \in \mathbb{Z}_p$ 与 $\alpha \in \mathbb{Z}_p$ 矛盾.

其他因子组合同理，都是计算次高项的系数，因为它一定是某些 $\alpha+i$ 的和都能得到 $\alpha \in \mathbb{Z}_p$ 这一矛盾.

□